CRYPTOLOGIA

Volume 36, Number 1, 2012

Space Crunchers and GOST Busters! 1
Craig Bauer

Security Evaluation of GOST 28147-89 in View of International Standardisation 2
Nicolas T. Courtois

The Pathology of Cryptology—A Current Survey 14
Klaus Schmeh

How to Scatter a Secret? 46
Eric Brier, Wenjie Fang, and David Naccache

The Flaw in the JN-25 Series of Ciphers, II 55
Peter Donovan

Security Flaws in Three Password-Based Remote User Authentication Schemes with Smart Cards 62
Kyung-Ah Shim

The XTS-AES Disk Encryption Algorithm and the Security of Ciphertext Stealing . . . 70
Matthew V. Ball, Cyril Guyot, James P. Hughes, Luther Martin, and Landon Curt Noll

Review of *The Mystic Cipher* by Dennis L. Mangrum 80
John F. Dooley

Volume 36, Number 2, 2012

100 Years Times Two: Alan Turing and the Voynich Manuscript 85
Craig Bauer

Lester Hill's Error-Detecting Codes 88
Chris Christensen, David Joyner, and Jenna Torres

On Integral Distinguishers of Rijndael Family of Ciphers 104
Marine Minier, Raphael C.-W. Phan, and Benjamin Pousse

Project Kalina: The Lotos Operation Conundrum 119
Jan Bury

Location Authentication, Tracking, and Emergency Signaling through Power Line Communication: Designs and Protocols for New Out-of-Band Strategies 129
Alan T. Sherman, Dhananjay Phatak, Vivek G. Relan, and Bhushan Sonawane

KRYPTOS: A Pacific Northwest Cryptanalysis Contest for Undergraduates 149
Cheryl Beaver and Stuart Boersma

Review of the 2011 Cryptologic History Symposium *Cryptology in War and Peace: Crisis Points in History* 157
Chris Christensen

Review of *Joe Rochefort's War* by Elliot Carlson 161
John F. Dooley

Review of *The Secrets of Station X—How the Bletchley Park Codebreakers Helped Win the War* by Michael Smith 164
David H. Hamer

Review of *Secret Days: Code-Breaking in Bletchley Park* by Asa Briggs 167
Chris Christensen

Review of *Neil Webster's Cribs for Victory* edited by Joss Pearson 173
Chris Christensen

Review of *In the Shadow of Pont du Gard: The Polish Enigma in Vichy France (June 1940 to November 1942)* by Zdzislaw J. Kapera 176
Chris Christensen

Review of *Inside Enigma: The Secrets of the Enigma Machine and Other Historic Cipher Machines* by Tom Perera 179
Chris Christensen

Review of *The Information: A History, A Theory, A Flood* by James Gleick 181
Chris Christensen

Review of *The Theory That Would Not Die* by Sharon McGrayne 183
David Agard and Chris Christensen

Volume 36, Number 3, 2012

Commentary on Alan M. Turing: The Applications of Probability to Cryptography . . 191
Sandy Zabell

Assembling the Puzzle Game: The Jacek Jurzak Spy Case 215
Jan Bury

Late 18th-Century French Encrypted Diplomatic "Letters of Recommendation"—Or, How to Unwittingly Carry Your Own Warrant 230
Gerhard F. Strasser

Statistics of Random Permutations and the Cryptanalysis of Periodic Block Ciphers. . 240
Gregory V. Bard, Shaun V. Ault, and Nicolas T. Courtois

A Cryptanalysis Service During the Spanish Civil War 263
José Ramón Soler Fuensanta, Francisco Javier López-Brea Espiau, and Diego Navarro Bonilla

First Charlotte International Cryptologic Symposium and Exhibit 290
David H. Hamer

Volume 36, Number 4, 2012

Report on Speech Secrecy System DELILAH, a Technical Description Compiled by A. M. Turing and Lieutenant D. Bayley REME, 1945–1946 295
Alan M. Turing and D. Bayley

Polish Cold War Codebreaking of 1959–1989: A Preliminary Assessment 341
Jan Bury

Annual Contents Listing